Docket No.: 60188-697 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 20277
Masahiro FUKUI, et al.	:	Confirmation Number:
Serial No.:	:	Group Art Unit:
Filed: November 19, 2003	:	Examiner:

For: CIRCUIT OPERATION SIMULATION APPARATUS

CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Mail Stop CPD
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. JP 2002-337898, filed on November 21, 2002.

cited in the Declaration of the present application. A certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Michael E. Fogarty
Registration No. 36,139

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 MEF:gav
Facsimile: (202) 756-8087
Date: November 19, 2003

60188-697
Masahiro Fukui, et al.
November 19, 2003

日　本　国　特　許　庁
JAPAN PATENT OFFICE

McDermott, Will & Emery

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年１１月２１日

出願番号
Application Number: 特願２００２－３３７８９８

[ST.10/C]: [ＪＰ２００２－３３７８９８]

出願人
Applicant(s): 松下電器産業株式会社

２００３年　１月１７日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００２－３１０６９１７

【書類名】　特許願
【整理番号】　2037640009
【提出日】　平成14年11月21日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 19/00
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　福井　正博
【発明者】
【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
【氏名】　徳永　祐介
【特許出願人】
【識別番号】　000005821
【氏名又は名称】　松下電器産業株式会社
【代理人】
【識別番号】　100077931
【弁理士】
【氏名又は名称】　前田　弘
【選任した代理人】
【識別番号】　100094134
【弁理士】
【氏名又は名称】　小山　廣毅
【選任した代理人】
【識別番号】　100110939
【弁理士】
【氏名又は名称】　竹内　宏

【選任した代理人】

【識別番号】　100110940

【弁理士】

【氏名又は名称】　嶋田　高久

【選任した代理人】

【識別番号】　100113262

【弁理士】

【氏名又は名称】　竹内　祐二

【選任した代理人】

【識別番号】　100115059

【弁理士】

【氏名又は名称】　今江　克実

【選任した代理人】

【識別番号】　100115510

【弁理士】

【氏名又は名称】　手島　勝

【選任した代理人】

【識別番号】　100115691

【弁理士】

【氏名又は名称】　藤田　篤史

【手数料の表示】

【予納台帳番号】　014409

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　0006010

【プルーフの要否】　要

【書類名】　　明細書

【発明の名称】　回路動作シミュレーション装置、回路動作シミュレーション方法、回路動作シミュレーションプログラム、および回路情報復号化プログラム

【特許請求の範囲】

【請求項１】

回路の構成および特性に関する回路情報に基づいて回路の動作のシミュレーションを行うシミュレーション手段と、

暗号化された上記回路情報を記憶する記憶手段と、

上記暗号化された回路情報を上記記憶手段から読み出して復号化し、上記シミュレーション手段に与える記憶回路情報復号化手段と、

を備えたことを特徴とする回路動作シミュレーション装置。

【請求項２】

請求項１の回路動作シミュレーション装置であって、さらに、

上記シミュレーション手段によるシミュレーション中に生成された中間データを、暗号化して上記記憶手段に記憶させる中間データ暗号化手段と、

上記暗号化して上記記憶手段に記憶された上記中間データを読み出して復号化し、上記シミュレーション手段に与える中間データ復号化手段と、

を備えたことを特徴とする回路動作シミュレーション装置。

【請求項３】

請求項２の回路動作シミュレーション装置であって、

上記記憶回路情報復号化手段と、上記中間データ復号化手段とが兼用されるように構成されていることを特徴とする回路動作シミュレーション装置。

【請求項４】

請求項２の回路動作シミュレーション装置であって、さらに、

上記記憶手段に記憶された上記中間データをシミュレーションの終了後に削除する中間データ削除手段を備えたことを特徴とする回路動作シミュレーション装置。

【請求項５】

請求項１の回路動作シミュレーション装置であって、さらに、

第１の暗号化手法により暗号化されて供給された回路情報を復号化する供給回路情報復号化手段と、

上記供給回路情報復号化手段によって復号化された回路情報を第２の暗号化手法により暗号化して、上記記憶手段に記憶させる記憶回路情報暗号化手段と、

を備えるとともに、

上記記憶回路情報復号化手段は、上記記憶回路情報暗号化手段によって暗号化された回路情報を復号化するように構成されていることを特徴とする回路動作シミュレーション装置。

【請求項６】

請求項５の回路動作シミュレーション装置であって、さらに、

上記シミュレーション手段によるシミュレーション中に生成された中間データを、暗号化して上記記憶手段に記憶させる中間データ暗号化手段と、

上記暗号化して上記記憶手段に記憶された上記中間データを読み出して復号化し、上記シミュレーション手段に与える中間データ復号化手段と、

を備えるとともに、

上記記憶回路情報暗号化手段と、上記中間データ暗号化手段とが兼用されるように構成されていることを特徴とする回路動作シミュレーション装置。

【請求項７】

回路の構成および特性に関する回路情報に基づいて回路の動作のシミュレーションを行うシミュレーション手段と、

暗号化された上記回路情報を記憶する記憶手段と、

を備えるとともに、

上記記憶手段から読み出された上記暗号化された回路情報を復号化して上記シミュレーション手段に与える記憶回路情報復号化手段を組み込み可能に構成されていることを特徴とする回路動作シミュレーション装置。

【請求項８】

回路の構成および特性に関する回路情報に基づいて回路の動作のシミュレーションを行うシミュレーションステップと、

暗号化されて記憶手段に記憶された上記回路情報を読み出して復号化し、上記

シミュレーションステップで用いられるようにする記憶回路情報復号化ステップと、

を有することを特徴とする回路動作シミュレーション方法。

【請求項９】

請求項８の回路動作シミュレーション方法であって、さらに、

上記シミュレーションステップによるシミュレーション中に生成された中間データを、暗号化して上記記憶手段に記憶させる中間データ暗号化ステップと、

上記暗号化して上記記憶手段に記憶された上記中間データを読み出して復号化し、上記シミュレーションステップで用いられるようにする中間データ復号化ステップと、

を有することを特徴とする回路動作シミュレーション方法。

【請求項１０】

請求項９の回路動作シミュレーション方法であって、さらに、

上記記憶手段に記憶された上記中間データをシミュレーションの終了後に削除する中間データ削除ステップを有することを特徴とする回路動作シミュレーション方法。

【請求項１１】

請求項８の回路動作シミュレーション方法であって、さらに、

第１の暗号化手法により暗号化されて供給された回路情報を復号化する供給回路情報復号化ステップと、

上記供給回路情報復号化ステップによって復号化された回路情報を第２の暗号化手法により暗号化して、上記記憶手段に記憶させる記憶回路情報暗号化ステップと、

を有するとともに、

上記記憶回路情報復号化ステップは、上記記憶回路情報暗号化ステップによって暗号化された回路情報を復号化することを特徴とする回路動作シミュレーション方法。

【請求項１２】

回路の構成および特性に関する回路情報に基づいて回路の動作のシミュレーシ

ョンを行うシミュレーションステップと、

暗号化されて記憶手段に記憶された上記回路情報を読み出して復号化し、上記シミュレーションステップで用いられるようにする記憶回路情報復号化ステップと、

をコンピュータに実行させることを特徴とする回路動作シミュレーションプログラム。

【請求項１３】

請求項１２の回路動作シミュレーションプログラムであって、さらに、

上記シミュレーションステップによるシミュレーション中に生成された中間データを、暗号化して上記記憶手段に記憶させる中間データ暗号化ステップと、

上記暗号化して上記記憶手段に記憶された上記中間データを読み出して復号化し、上記シミュレーションステップで用いられるようにする中間データ復号化ステップと、

をコンピュータに実行させることを特徴とする回路動作シミュレーションプログラム。

【請求項１４】

請求項１３の回路動作シミュレーションプログラムであって、さらに、

上記記憶手段に記憶された上記中間データをシミュレーションの終了後に削除する中間データ削除ステップをコンピュータに実行させることを特徴とする回路動作シミュレーションプログラム。

【請求項１５】

請求項１２の回路動作シミュレーションプログラムであって、さらに、

第１の暗号化手法により暗号化されて供給された回路情報を復号化する供給回路情報復号化ステップと、

上記供給回路情報復号化ステップによって復号化された回路情報を第２の暗号化手法により暗号化して、上記記憶手段に記憶させる記憶回路情報暗号化ステップと、

を有するとともに、

上記記憶回路情報復号化ステップは、上記記憶回路情報暗号化ステップによっ

て暗号化された回路情報を復号化するように構成されていることを特徴とする回路動作シミュレーションプログラム。

【請求項１６】

回路の構成および特性に関する回路情報に基づいて回路の動作のシミュレーションを行うシミュレーションステップをコンピュータに実行させる回路動作シミュレーションプログラムであって、

暗号化されて記憶手段に記憶され、読み出された上記回路情報を復号化して上記シミュレーションステップで用いられるようにする組込用復号化プログラムを組み込み可能に構成されていることを特徴とする回路動作シミュレーションプログラム。

【請求項１７】

暗号化されて記憶手段に記憶された、回路の構成および特性に関する回路情報を読み出して復号化する記憶回路情報復号化ステップをコンピュータに実行させる回路情報復号化プログラムであって、

回路情報に基づいて回路の動作のシミュレーションを行うシミュレーションステップをコンピュータに実行させる回路動作シミュレーションプログラムに組み込まれることによって、上記復号化された回路情報が上記シミュレーションステップで用いられるように構成されていることを特徴とする回路情報復号化プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、電子回路、特に半導体集積回路を用いた電子回路の動作のシミュレーションを行う回路動作シミュレーション装置に関する技術に属するものである。

【０００２】

【従来の技術】

従来より、電子回路の設計や動作の検証などをするために、回路動作シミュレーション装置が用いられている。具体的には、例えば回路ライブラリなどとして

記憶部に記憶された回路情報と、回路への入力信号などを示すシミュレーション入力データとに基づいて、各部の信号レベルを求めることにより、回路動作のシミュレーションが行われるようになっている（例えば、特許文献１参照）。また、シミュレーションされる電子回路に、他の製造元から供給される半導体集積回路が含まれる場合、その半導体集積回路についての回路情報は、製造元から提供を受けて、他の（周辺回路などの）回路情報と共に記憶部に記憶させることにより、電子回路全体の回路動作のシミュレーションが行われる。これによって、半導体集積回路の動作も含む全体の動作や機能（入出力信号の関係や内部状態等）の検証や、周辺回路の最適化などを行うことができる。

【０００３】

ここで、上記回路動作のシミュレーションに用いられる回路情報には、例えば回路を構成する各素子の特性を示す情報や、各素子間の接続関係を示す情報などが含まれている。また、回路情報の表現形式としては、通常、業界で標準的に用いられる書式に従ったテキストデータなどの形式、具体的には、例えばSPICEと称される装置等に代表されるシミュレータ用のソースリスト形式や、Verilog-HDLに代表される機能記述言語形式、また、レイアウトデータ形式等が用いられる。すなわち、公開された一定の規則に従って記述された回路情報が用いられることにより、多くの回路動作シミュレーション装置において、半導体集積回路の製造元から提供される回路情報に基づいたシミュレーションを行い得るようになっている。

【０００４】

【特許文献１】

特開平８－１８００８８号公報

【０００５】

【発明が解決しようとする課題】

上記従来の回路動作シミュレーション装置では、上記のように標準的に用いられる形式の回路情報に基づいてシミュレーションを行えるようにすることにより、種々の製造元から提供される半導体集積回路を用いた電子回路の動作のシミュレーションをすることができるものの、上記のような形式の回路情報は、公開さ

れた一定の規則に従って記述されたものであるため、提供を受けた側などが回路情報を解読することによって、半導体集積回路に用いられている素子の種類や各素子の接続関係、すなわち回路設計上のノウハウや開発傾向などの設計情報を容易に把握することが可能である。そこで、一般に、ＮＤＡ（Non-Disclosure Agreement）等と称される秘密保持契約の下に、半導体集積回路の回路情報の提供がなされている。しかし、この種の契約は、法律的処理等に要する労力が非常に大きいため、半導体集積回路やこれを用いた製品などの製造コストを増大させる要因となる。また、提供を受ける側には、示された回路情報に関連する技術については独自に開発することが禁止されるなどのリスクが伴う。それゆえ、半導体集積回路を含む回路のシミュレーションは、その半導体集積回路の適用される蓋然性が高い場合でなければ、実際上、容易に行うことができない。

【０００６】

本発明は、上記の点に鑑み、回路情報の秘匿性を守りつつ、回路動作シミュレーション装置によってシミュレーションを容易に行えるようにすることを課題とする。

【０００７】

【課題を解決するための手段】

上記の課題を解決するために、請求項１の発明が講じた解決手段は、

回路動作シミュレーション装置であって、

回路の構成および特性に関する回路情報に基づいて回路の動作のシミュレーションを行うシミュレーション手段と、

暗号化された上記回路情報を記憶する記憶手段と、

上記暗号化された回路情報を上記記憶手段から読み出して復号化し、上記シミュレーション手段に与える記憶回路情報復号化手段と、

を備えたことを特徴とする。

【０００８】

これにより、回路動作をシミュレーションするための回路情報を暗号化した状態で提供できるので、秘匿性を保つことができ、したがって、インターネットを利用したり仲介者を介したりするなど、柔軟な形態で回路情報を提供することが

できる。また、ユーザが記憶手段の記憶内容を不用意に見てしまっても、回路情報を知ることはできず、秘匿性が保たれるので、特にＮＤＡなどの契約を結ぶ必要はなく、手軽にシミュレーションすることができる。

【０００９】

また、請求項２の発明は、

請求項１の回路動作シミュレーション装置であって、さらに、

上記シミュレーション手段によるシミュレーション中に生成された中間データを、暗号化して上記記憶手段に記憶させる中間データ暗号化手段と、

上記暗号化して上記記憶手段に記憶された上記中間データを読み出して復号化し、上記シミュレーション手段に与える中間データ復号化手段と、

を備えたことを特徴とする。

【００１０】

これにより、ユーザが中間データに基づいて実質的に回路情報を知ってしまうことがないので、やはり、回路情報の秘匿性を容易に保つことができる。特に、シミュレーションがエラーにより異常終了して中間データが記憶手段に残っているような場合などでも、回路情報の秘匿性を保つことができる。

【００１１】

また、請求項３の発明は、

請求項２の回路動作シミュレーション装置であって、

上記記憶回路情報復号化手段と、上記中間データ復号化手段とが兼用されるように構成されていることを特徴とする。

【００１２】

これにより、装置の構成の簡素化を図ることができる。

【００１３】

また、請求項４の発明は、

請求項２の回路動作シミュレーション装置であって、さらに、

上記記憶手段に記憶された上記中間データをシミュレーションの終了後に削除する中間データ削除手段を備えたことを特徴とする。

【００１４】

これにより、シミュレーションの終了後に、回路動作シミュレーション装置の利用者が記憶手段の記憶内容を不用意に見てしまうことによって回路情報が知られることを防止することができる。

【００１５】

また、請求項５の発明は、

請求項１の回路動作シミュレーション装置であって、さらに、

第１の暗号化手法により暗号化されて供給された回路情報を復号化する供給回路情報復号化手段と、

上記供給回路情報復号化手段によって復号化された回路情報を第２の暗号化手法により暗号化して、上記記憶手段に記憶させる記憶回路情報暗号化手段と、

を備えるとともに、

上記記憶回路情報復号化手段は、上記記憶回路情報暗号化手段によって暗号化された回路情報を復号化するように構成されていることを特徴とする。

【００１６】

これにより、回路情報が供給される際の暗号化と、記憶手段に記憶される際の暗号化とを分けて、インターネットなどを介した流通段階での秘匿性を高める一方、シミュレーションのための復号化の高速化を図ることができる。

【００１７】

また、請求項６の発明は、

請求項５の回路動作シミュレーション装置であって、さらに、

上記シミュレーション手段によるシミュレーション中に生成された中間データを、暗号化して上記記憶手段に記憶させる中間データ暗号化手段と、

上記暗号化して上記記憶手段に記憶された上記中間データを読み出して復号化し、上記シミュレーション手段に与える中間データ復号化手段と、

を備えるとともに、

上記記憶回路情報暗号化手段と、上記中間データ暗号化手段とが兼用されるように構成されていることを特徴とする。

【００１８】

これにより、前記のように流通段階での秘匿性とシミュレーションの高速化を

図るとともに、装置の構成の簡素化を図ることができる。

【００１９】

また、請求項７の発明は、

回路動作シミュレーション装置であって、

回路の構成および特性に関する回路情報に基づいて回路の動作のシミュレーションを行うシミュレーション手段と、

暗号化された上記回路情報を記憶する記憶手段と、

を備えるとともに、

上記記憶手段から読み出された上記暗号化された回路情報を復号化して上記シミュレーション手段に与える記憶回路情報復号化手段を組み込み可能に構成されていることを特徴とする。

【００２０】

これにより、前記のように暗号化によって回路情報の秘匿性を高め得る回路動作シミュレーション装置を容易に構成することができる。

【００２１】

また、請求項８の発明は、

回路動作シミュレーション方法であって、

回路の構成および特性に関する回路情報に基づいて回路の動作のシミュレーションを行うシミュレーションステップと、

暗号化されて記憶手段に記憶された上記回路情報を読み出して復号化し、上記シミュレーションステップで用いられるようにする記憶回路情報復号化ステップと、

を有することを特徴とする。

【００２２】

また、請求項９の発明は、

請求項８の回路動作シミュレーション方法であって、さらに、

上記シミュレーションステップによるシミュレーション中に生成された中間データを、暗号化して上記記憶手段に記憶させる中間データ暗号化ステップと、

上記暗号化して上記記憶手段に記憶された上記中間データを読み出して復号化

し、上記シミュレーションステップで用いられるようにする中間データ復号化ステップと、

を有することを特徴とする。

【００２３】

また、請求項１０の発明は、

請求項９の回路動作シミュレーション方法であって、さらに、

上記記憶手段に記憶された上記中間データをシミュレーションの終了後に削除する中間データ削除ステップを有することを特徴とする。

【００２４】

また、請求項１１の発明は、

請求項８の回路動作シミュレーション方法であって、さらに、

第１の暗号化手法により暗号化されて供給された回路情報を復号化する供給回路情報復号化ステップと、

上記供給回路情報復号化ステップによって復号化された回路情報を第２の暗号化手法により暗号化して、上記記憶手段に記憶させる記憶回路情報暗号化ステップと、

を有するとともに、

上記記憶回路情報復号化ステップは、上記記憶回路情報暗号化ステップによって暗号化された回路情報を復号化することを特徴とする。

【００２５】

また、請求項１２の発明は、

回路動作シミュレーションプログラムであって、

回路の構成および特性に関する回路情報に基づいて回路の動作のシミュレーションを行うシミュレーションステップと、

暗号化されて記憶手段に記憶された上記回路情報を読み出して復号化し、上記シミュレーションステップで用いられるようにする記憶回路情報復号化ステップと、

をコンピュータに実行させることを特徴とする。

【００２６】

また、請求項１３の発明は、

請求項１２の回路動作シミュレーションプログラムであって、さらに、

上記シミュレーションステップによるシミュレーション中に生成された中間データを、暗号化して上記記憶手段に記憶させる中間データ暗号化ステップと、

上記暗号化して上記記憶手段に記憶された上記中間データを読み出して復号化し、上記シミュレーションステップで用いられるようにする中間データ復号化ステップと、

をコンピュータに実行させることを特徴とする。

【００２７】

また、請求項１４の発明は、

請求項１３の回路動作シミュレーションプログラムであって、さらに、

上記記憶手段に記憶された上記中間データをシミュレーションの終了後に削除する中間データ削除ステップをコンピュータに実行させることを特徴とする。

【００２８】

また、請求項１５の発明は、

請求項１２の回路動作シミュレーションプログラムであって、さらに、

第１の暗号化手法により暗号化されて供給された回路情報を復号化する供給回路情報復号化ステップと、

上記供給回路情報復号化ステップによって復号化された回路情報を第２の暗号化手法により暗号化して、上記記憶手段に記憶させる記憶回路情報暗号化ステップと、

を有するとともに、

上記記憶回路情報復号化ステップは、上記記憶回路情報暗号化ステップによって暗号化された回路情報を復号化するように構成されていることを特徴とする。

【００２９】

これらにより、やはり、回路動作をシミュレーションするための回路情報を暗号化した状態で提供できるので、秘匿性を保つことができ、したがって、インターネットを利用したり仲介者を介したりするなど、柔軟な形態で回路情報を提供することができる。また、ユーザが記憶手段の記憶内容を不用意に見てしまって

も、回路情報を知ることはできず、秘匿性が保たれるので、特にＮＤＡなどの契約を結ぶ必要はなく、手軽にシミュレーションすることができる。

【００３０】

また、ユーザが中間データに基づいて実質的に回路情報を知ってしまうことがないので、やはり、回路情報の秘匿性を容易に保つことができる。特に、シミュレーションがエラーにより異常終了して中間データが記憶手段に残っているような場合などでも、回路情報の秘匿性を保つことができる。

【００３１】

また、シミュレーションの終了後に、回路動作シミュレーション装置の利用者が記憶手段の記憶内容を不用意に見てしまうことによって回路情報が知られることを防止することができる。

【００３２】

また、回路情報が供給される際の暗号化と、記憶手段に記憶される際の暗号化とを分けて、インターネットなどを介した流通段階での秘匿性を高める一方、シミュレーションのための復号化の高速化を図ることができる。

【００３３】

また、請求項１６の発明は、

回路の構成および特性に関する回路情報に基づいて回路の動作のシミュレーションを行うシミュレーションステップをコンピュータに実行させる回路動作シミュレーションプログラムであって、

暗号化されて記憶手段に記憶され、読み出された上記回路情報を復号化して上記シミュレーションステップで用いられるようにする組込用復号化プログラムを組み込み可能に構成されていることを特徴とする。

【００３４】

また、請求項１７の発明は、

回路情報復号化プログラムであって、

暗号化されて記憶手段に記憶された、回路の構成および特性に関する回路情報を読み出して復号化する記憶回路情報復号化ステップをコンピュータに実行させる回路情報復号化プログラムであって、

回路情報に基づいて回路の動作のシミュレーションを行うシミュレーションステップをコンピュータに実行させる回路動作シミュレーションプログラムに組み込まれることによって、上記復号化された回路情報が上記シミュレーションステップで用いられるように構成されていることを特徴とする。

【００３５】

これらにより、やはり、前記のように暗号化によって回路情報の秘匿性を高め得る回路動作シミュレーション装置を容易に構成することができる。

【００３６】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照しながら説明する。

【００３７】

図１は回路動作シミュレーション装置１００の要部の構成を示すブロック図である。同図において、

供給回路情報復号化部１０１（供給回路情報復号化手段）は、暗号化された回路情報である供給回路情報、暗号化復号化アルゴリズムデータ（暗号化や復号化に用いられる関数、プログラム、またはルーチンなど）、およびキーデータ（復号化演算をする際の初期値やパスワードなど）に基づいて、上記供給回路情報を復号化し、平文の回路情報を生成するようになっている。

【００３８】

記憶回路情報暗号化部１０２（記憶回路情報暗号化手段）は、供給回路情報復号化部１０１によって復号化された回路情報をさらに暗号化して、記憶回路情報を生成するようになっている。この暗号化は、例えば変換テーブル１０２ａに基づいたデータの変換によって行われる。より詳しくは、平文の回路情報に対して、例えば図２に示すような各バイトデータと１対１で対応したバイトデータへの変換や、補数化演算、隣り合うバイトデータごとの排他的論理和演算、ビット並びの並べ替えなどを施すことによる暗号化が行われる。すなわち、供給回路情報に比べて暗号化強度は低くても高速な暗号化や復号化が容易な方式で暗号化されるようになっている。

【００３９】

記憶部１０３（記憶手段）は、上記暗号化された記憶回路情報や、回路動作シミュレーション装置の利用者などが作成した平文の回路情報、シミュレーション過程における中間データ（テンポラリファイルやテンポラリデータ）などを記憶するものである。この記憶部１０３は、具体的には、ハードディスクドライブ（ＨＤＤ）やメモリなどによって構成される。上記暗号化された記憶回路情報と平文の回路情報との判別方法は、特に限定されないが、例えば各行の先頭に記号「＊」が付されているかどうかや所定のビットの値等によって容易に判別できるようになっている。なお、記憶部１０３には、前記供給回路情報復号化部１０１に与えられる供給回路情報や、暗号化復号化アルゴリズムデータ、キーデータも一旦保持されるようにしてもよい。

【００４０】

記憶回路情報・中間データ復号化部１０４（記憶回路情報復号化手段、中間データ復号化手段）は、記憶部１０３に記憶された、暗号化された記憶回路情報や中間データを復号化するようになっている。上記復号化は、例えば記憶回路情報暗号化部１０２の変換テーブル１０２ａと同一または対応する変換テーブル１０４ａに基づいて行われる。

【００４１】

シミュレータエンジン１０５（シミュレーション手段）は、記憶回路情報・中間データ復号化部１０４から出力される復号化された回路情報等に基づいて、回路動作のシミュレーションを行うようになっている。

【００４２】

中間データ暗号化部１０６（中間データ暗号化手段）は、シミュレータエンジン１０５からシミュレーションの実行中に出力される中間データを変換テーブル１０２ａと同一の変換テーブル１０６ａに基づいて暗号化し、記憶部１０３に記憶させるようになっている。

【００４３】

上記のような回路動作シミュレーション装置は、具体的には、例えば記憶部１０３を有するコンピュータと、その他の各部に対応するソフトウェアとによって構成されるが、これに限らず、少なくとも一部がハードウェアによって構成され

るなどしてもよい。また、ソフトウェアを用いて記憶回路情報・中間データ復号化部１０４等を構成する場合には、シミュレータエンジン１０５等の機能を拡張するプラグインやアドオンなどの形式を用いるようにしてもよい。この場合には、例えばシミュレータエンジン１０５にプラグインを組み込み得る仕組みを設けるだけで、容易に、回路動作シミュレーション装置の機能を拡張して上記のような回路情報の暗号化、復号化機能を持たせることができるとともに、シミュレータエンジン１０５やプラグインに汎用性を持たせることもできる。また、既存のシミュレータエンジンの入出力ルーチン等をフックして上記のような機能を持たせるソフトウェアを用いるなどしてもよい。なお、回路動作シミュレーション装置には、一般的に、上記の他に入力装置や表示装置なども備えられるが、以下の説明では省略する。

【００４４】

上記のように構成された回路動作シミュレーション装置によってシミュレーションが行われる際には、まず、供給回路情報復号化部１０１が、供給回路情報、暗号化復号化アルゴリズムデータ、およびキーデータに基づいて、平文の回路情報を生成する。また、記憶回路情報暗号化部１０２は、上記平文の回路情報を変換テーブル１０２ａに基づいて暗号化し、生成された記憶回路情報を記憶部１０３に記憶させる。ここで、上記供給回路情報復号化部１０１による復号化と記憶回路情報暗号化部１０２による暗号化とは連続的に行われる。すなわち、例えばコンピュータのプロセッサ内で復号化された回路情報は、直ちに記憶回路情報に変換され、平文の回路情報全体などがファイルのような明示的な形で記憶部１０３に保持されたりしないようになっている。これにより、記憶部１０３に記憶されているファイルの読み出しやメモリダンプなどの一般的な手法によっては、平文の回路情報を知ることができない。

【００４５】

上記のようにして記憶部１０３に記憶された記憶回路情報および後述する中間データは、シミュレータエンジン１０５によって参照される際には、記憶回路情報・中間データ復号化部１０４によって復号化される。また、平文のままで記憶された回路情報は、そのままシミュレータエンジン１０５に出力される。

【００４６】

シミュレータエンジン１０５は、記憶回路情報・中間データ復号化部１０４から入力される平文のデータに基づいてシミュレーションを行う。すなわち、記憶部１０３に記憶されているデータが暗号化されていても、シミュレータエンジン１０５には復号化された平文のデータが入力されるので、シミュレータエンジン１０５自体には従来の装置と同様の動作をさせるだけでよい。上記シミュレーションによる結果は、表示装置に表示されるなどして、回路動作シミュレーション装置の利用者に提示される。また、シミュレーション過程で生成される中間データは、記憶部１０３には直接記憶されずに、中間データ暗号化部１０６に出力され、記憶回路情報暗号化部１０２と同じ手法で暗号化されてから記憶される。この中間データがシミュレータエンジン１０５によって参照される場合には、上記のように記憶回路情報・中間データ復号化部１０４による復号化が行われる。

【００４７】

また、シミュレーションが終了する際には、シミュレータエンジン１０５または図示しない削除部（中間データ削除手段）によって、記憶部１０３に記憶された中間データが全て削除される。この削除は、単なるメモリの領域の解放やファイル管理情報の削除を行うだけでなく、記憶されたデータの実体をダミーデータやゼロデータ等で上書きして抹消することが好ましい。なお、このような削除が行われる場合には、必ずしも中間データを暗号化しなくてもよく、この場合でも、ある程度の秘匿性を得ることができるが、中間データを暗号化する場合には、シミュレーション中にエラーが生じるなどの不慮の事故があった場合や、シミュレーションが終了しない時点でテンポラリファイルやメモリ内のデータを参照される場合などでも、秘匿性を確保することが容易にできる。

【００４８】

上記のように、回路動作シミュレーション装置に与えられる供給回路情報が暗号化されていることによって、回路情報が半導体集積回路の製造元などから回路動作シミュレーション装置の利用者に届くまでの間に第三者（特に悪意の者）に漏洩することを防止することができるとともに（第１の秘匿化）、記憶部１０３に記憶される記憶回路情報と中間データとが暗号化されていることによって、回

路情報が装置の利用者に知られてしまうことを防止することができる（第２の秘匿化）。

【００４９】

すなわち、第１の秘匿化に関しては、供給回路情報復号化部１０１による供給回路情報の復号化が、供給回路情報、暗号化復号化アルゴリズムデータ、およびキーデータに基づいて行われるので、少なくとも何れか１つのデータが第三者に入手できないような方法で伝送されることによって、容易に回路情報の漏洩が防止される。具体的には、例えばデータの伝送形態として、専用回線による接続や、郵送による方法などを用いることによって、容易に秘匿性を確保することができる。また、インターネットを利用したＶＰＮ（Virtual Private Network）やＩＰｓｅｃ（Security Architecture for Internet Protocol）、または公衆回線を用いたダイヤルアップ接続等によるＰＰＰ（Point to Point Protocol）を用いるとともに、受取人が正規の利用者であることをパスワードなどによって認証するようにすることもできる。特に、頻繁に伝送する必要性の少ない暗号化復号化アルゴリズムデータおよび／またはキーデータが上記のような経路で伝送されていれば、供給回路情報は、図３に示すようにインターネットを介したＨＴＴＰ（HyperText Transfer Protocol）やＦＴＰ（File Transfer Protocol）によって伝送することもできる。それゆえ、秘匿性を損なうことなく、種々の半導体集積回路などを用いた回路についてのシミュレーションを容易に行うことができる。また、例えば図４に示すように、供給回路情報、暗号化復号化アルゴリズムデータ、およびキーデータ、またはこれらのうちの少なくとも一部を回路情報または半導体集積回路の仲介者や仲介者側のサーバ装置などを介して提供させることも容易にできる。すなわち、回路情報の秘匿性を損なうことなく、流通や管理の利便性を向上させることができる。また、回路動作シミュレーション装置や、供給回路情報復号化部１０１等、および暗号化復号化アルゴリズムデータの作成者が回路情報の提供者と異なる場合などでも、回路情報の秘匿性を損なわないようにすることができる。

【００５０】

ここで、暗号化の方法は特に限定されるものではなく、例えば種々の秘密鍵暗

号方式や、公開鍵暗号方式、また、キーデータを用いずに暗号化復号化アルゴリズムデータだけを用いて暗号化復号化を行う方式を用いるようにしてもよい。さらに、供給回路情報等をインターネットを介したＳＳＬ（Secure Socket Layer）を用いて伝送するようにしてもよい。ただし、その場合には、トランスポート層以上のレイヤによる処理結果が記憶回路情報暗号化部１０２だけに与えられるように、専用のトランスポート層等の処理部を設けることが好ましい。

【００５１】

一方、第２の秘匿化に関しては、記憶部１０３に記憶される記憶回路情報や中間データが暗号化されていることによって、メモリダンプが行われたり、シミュレータエンジン１０５以外のプログラムによってファイルが開かれたりしたとしても、その内容が復号化（解読）されなければ、回路情報を回路動作シミュレーション装置の利用者に知られることはない。すなわち、利用者が意図的に回路情報を不正取得しようとするのでなければ、回路情報が利用者の目に触れることはないので、ＮＤＡ等の秘密保持契約などを結ぶ必要がない。それゆえ、利用者は秘密保持義務などの制約を受けることなく、手軽に充分なシミュレーションを行うことができるとともに、回路情報の漏洩が防止される。ただし、記憶回路情報等の解読や他者への配布がなされないことを担保するためには、そのような行為をしないことを約する契約等を結ぶことが好ましいが、そのような契約等は、利用者に特に制約を与えるものではなく、また、一般に厳格な手続きを必要としないため、契約を結びやすいうえ、仲介者による契約代行なども容易になるので、やはり、簡便にシミュレーションを行えるようにすることができる。

【００５２】

なお、上記の例では、暗号化復号化アルゴリズムデータが回路動作シミュレーション装置の外部から供給される例を示したが、これに限らず、あらかじめ回路動作シミュレーション装置や供給回路情報復号化部１０１等に組み込まれるようにしてもよい。ただし、上記のように外部から供給されるようにする場合には、必要に応じて最新の暗号化技術を適用することなどが容易にできる。また、供給回路情報またはそのグループや、供給回路情報の利用者などに対応させてアルゴリズムを異ならせることによって、機密管理の柔軟性を高めることなども容易に

できる。また、キーデータに関しても、各供給回路情報ごとに異ならせるようにしてもよいし、供給回路情報のグループや利用者などに対応させて異ならせるようにしてもよい。

【００５３】

また、上記の例では、記憶回路情報暗号化部１０２、記憶回路情報・中間データ復号化部１０４、および中間データ暗号化部１０６にそれぞれ変換テーブル１０２ａ・１０４ａ・１０６ａが設けられる例を示したが、これらの共通化を図るようにしてもよい。また、このような変換テーブルを用いる暗号化、複合化方式は一般に処理速度の点で有利であるが、これに限らず、供給回路情報の暗号化について説明したような種々の暗号化方式などを用いるようにしてもよい。特に、供給回路情報に対応する暗号化方式が用いられる場合には、供給回路情報復号化部１０１や記憶回路情報暗号化部１０２を設けることなく、提供された供給回路情報が直接記憶回路情報・中間データ復号化部１０４によって復号化されるようにしてもよい。また、暗号化テーブル等が用いられる場合、これらも、固定的に設けられるのに限らず、外部から供給されるようにしてもよい。この場合、変換テーブル等は、回路情報と共に暗号化されて供給回路情報に含められるなどしてもよい。

【００５４】

また、供給回路情報や、記憶回路情報暗号化部１０２や中間データ暗号化部１０６によって暗号化される記憶回路情報は、必ずしも全てのデータが暗号化されるのに限らず、少なくとも、機密が必要な内容に対して部分的に暗号化されるようにしてもよい。具体的には、例えば回路を構成する素子の特性、または素子の接続関係の何れか一方だけにノウハウがあるある場合にはその素子の特性または接続関係に関連するデータだけが暗号化されるようにしてもよい。

【００５５】

また、記憶回路情報暗号化部１０２と中間データ暗号化部１０６とは、別個に設けるのに限らず、兼用されるようにして、構成の簡素化を図り得るようにしてもよい。さらに、暗号化演算手法と復号化演算手法とが実質的に同一である場合（同じ演算を２回行うと元のデータに戻るような場合）には、記憶回路情報・中

間データ復号化部１０４も兼用されるようにしてもよい。

【００５６】

また、回路情報の提供者側で、回路情報に対して、記憶回路情報暗号化部１０２で生成される記憶回路情報と同様の暗号化が施された後に、さらに供給回路情報復号化部１０１に対応する暗号化が施されたものが、供給回路情報として提供されるようにしてもよい。この場合には、記憶回路情報暗号化部１０２を設けることなく、供給回路情報復号化部１０１によって復号化された記憶回路情報をそのまま記憶部１０３に記憶させるようにすることができ、供給回路情報復号化部１０１として通常の復号化プログラムを用いたり、自己解凍形式の供給回路情報を用いたりすることもできる。

【００５７】

【発明の効果】

以上のように本発明によると、回路情報やシミュレーション過程での中間データが暗号化されて記憶部に記憶され、読み出される際に復号化されてシミュレーションが行われるようにすることにより、第三者に回路情報を知られてしまうことや、回路動作シミュレーション装置の利用者が不用意に回路情報を知ってしまうのを防止することができ、回路情報の秘匿性を守りつつ、容易にシミュレーションを行うことができる。したがって、回路情報や半導体集積回路などの流通や管理の柔軟性を高めて、容易に流通等させることができる。

【図面の簡単な説明】

【図１】

本発明の実施の形態の回路動作シミュレーション装置の要部の構成を示すブロック図である。

【図２】

同、記憶回路情報暗号化部１０２等による暗号化、復号化方法の例を示す説明図である。

【図３】

同、供給回路情報等の伝送形態の例を示す説明図である。

【図４】

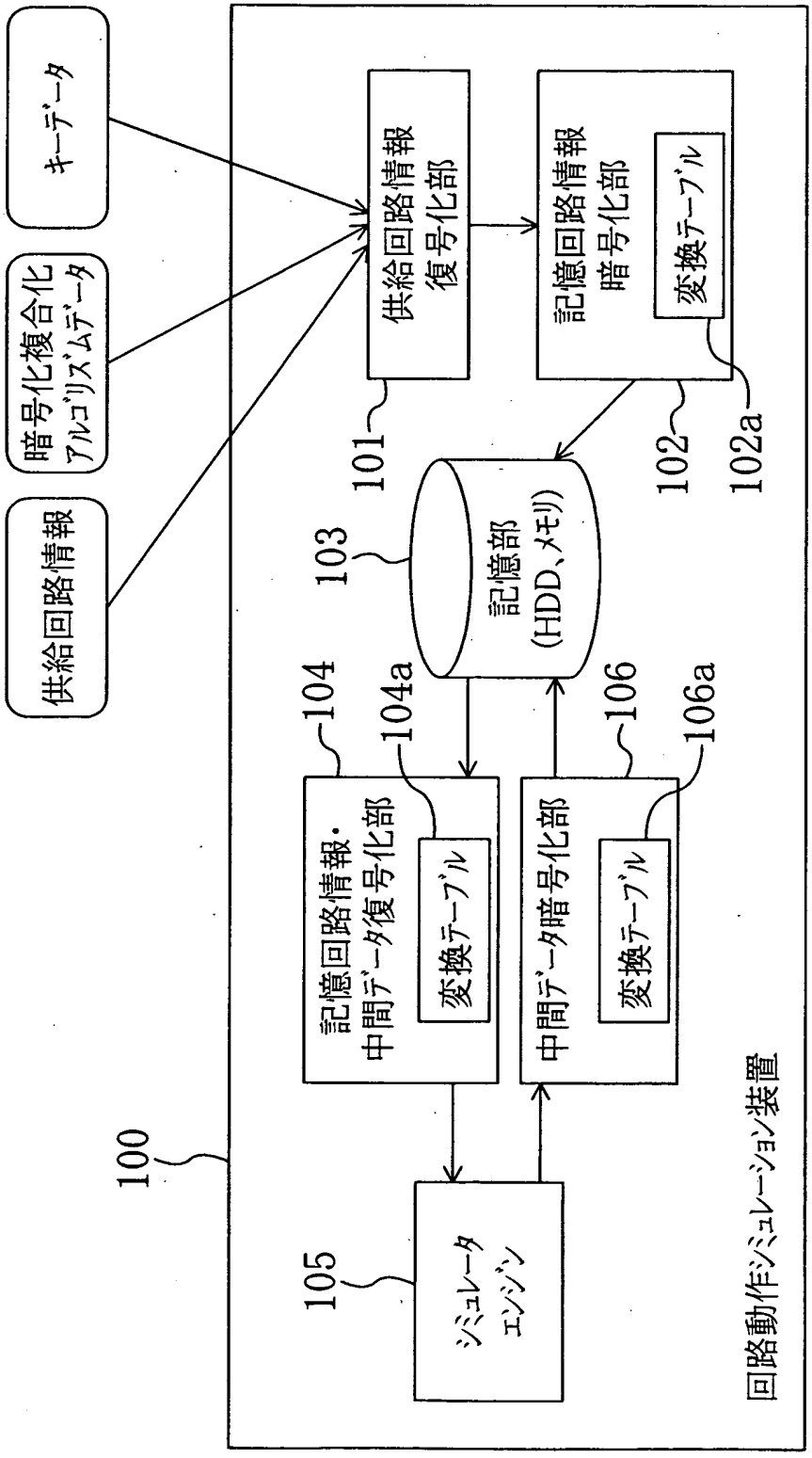
同、供給回路情報等の伝送形態の他の例を示す説明図である。

【符号の説明】

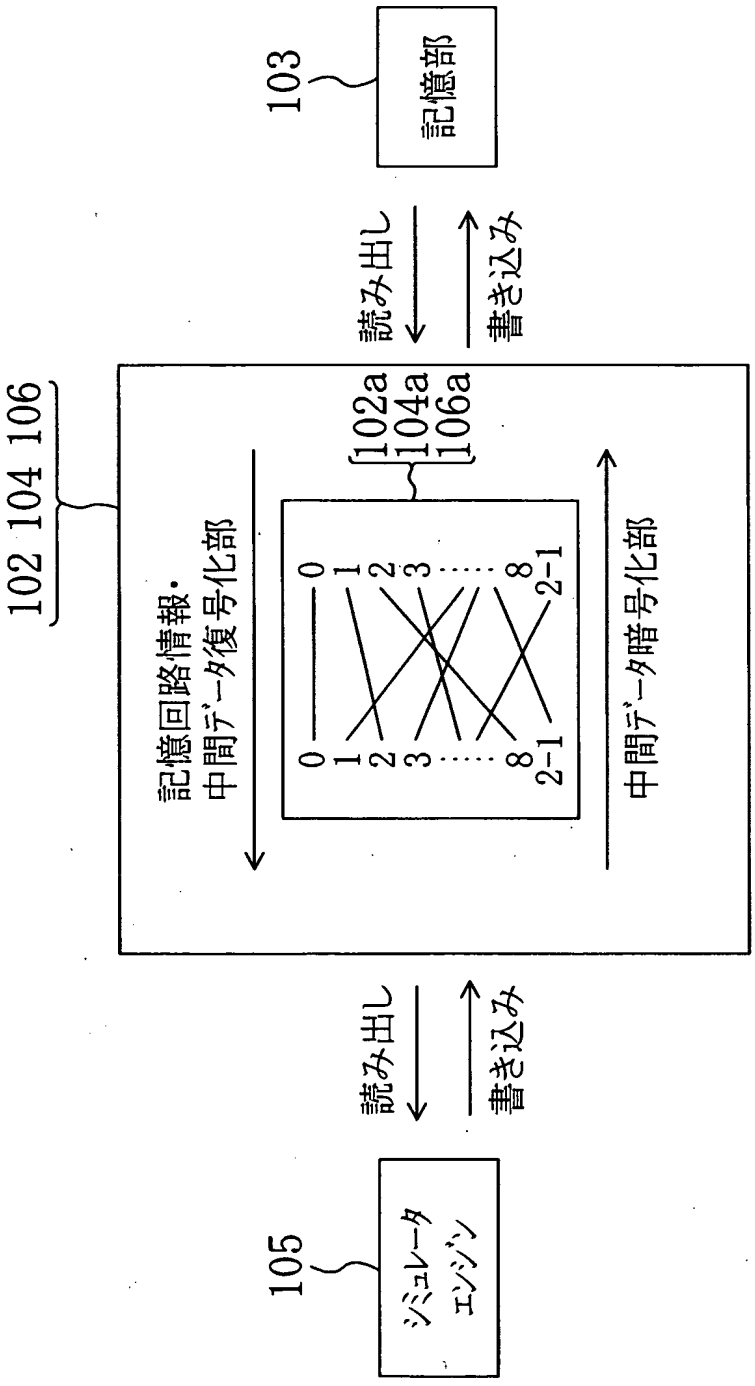
１００	回路動作シミュレーション装置
１０１	供給回路情報復号化部
１０２	記憶回路情報暗号化部
１０２ａ	変換テーブル
１０３	記憶部
１０４	記憶回路情報・中間データ復号化部
１０４ａ	変換テーブル
１０５	シミュレータエンジン
１０６	中間データ暗号化部
１０６ａ	変換テーブル

【書類名】　　図面

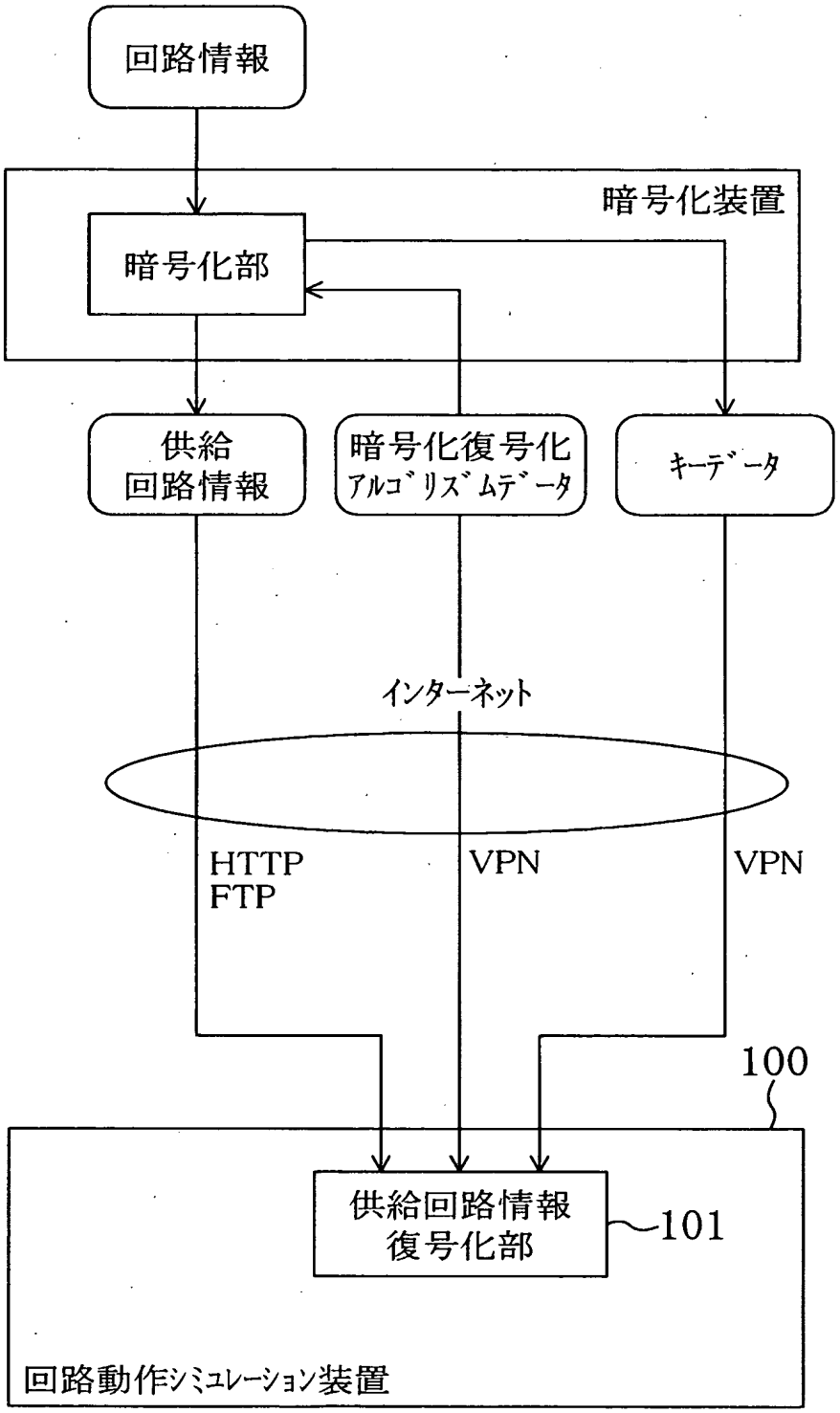
【図１】


キーデータ
暗号化複合化アルゴリズムデータ
供給回路情報
供給回路情報復号化部
記憶回路情報暗号化部
変換テーブル
101
102
102a
103
記憶部(HDD、メモリ)
104
104a
106
106a
記憶回路情報・中間データ復号化部
変換テーブル
中間データ暗号化部
変換テーブル
105
シミュレータエンジン
100
回路動作シミュレーション装置

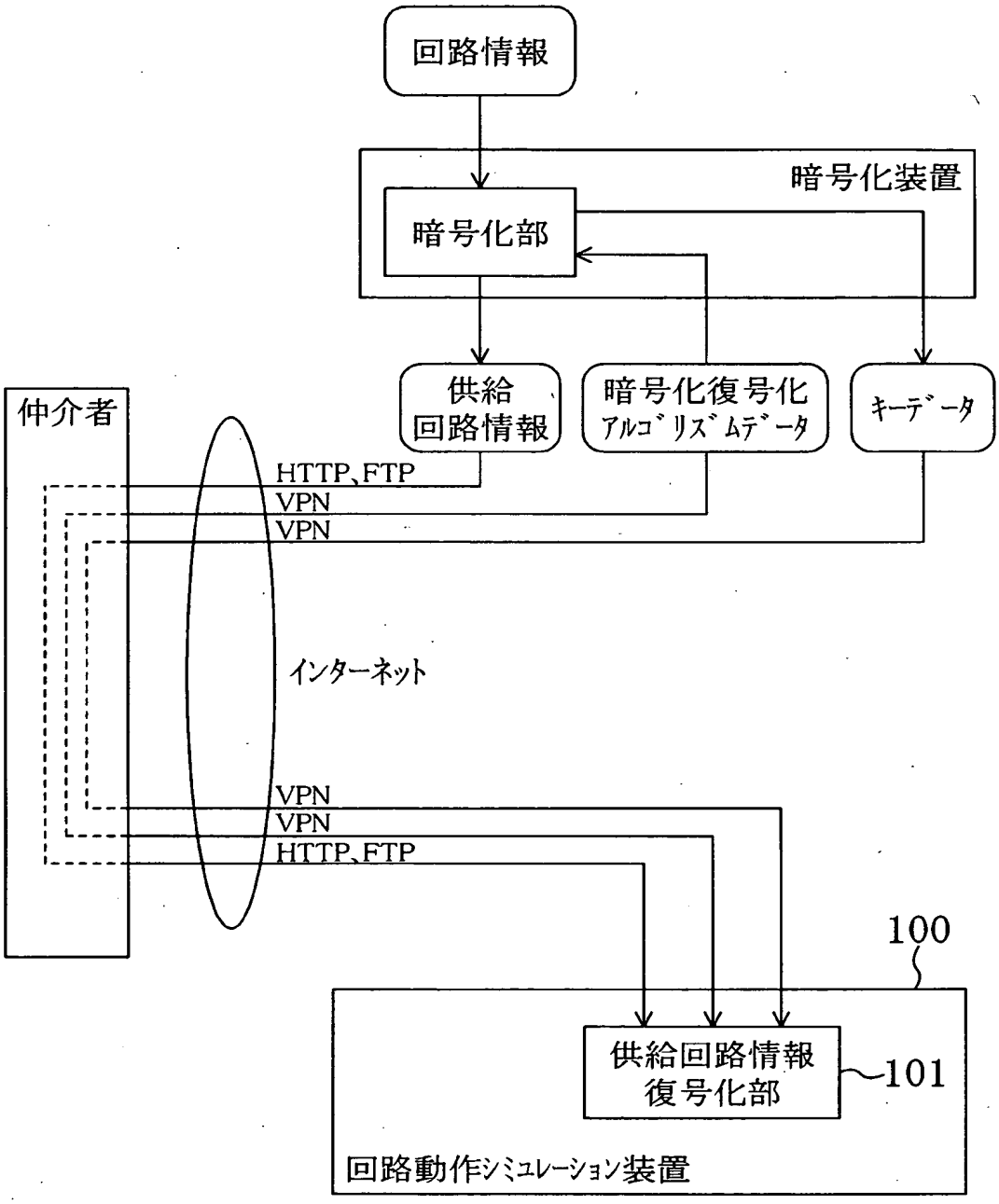
【図２】


103
記憶部
読み出し
書き込み
102 104 106
102a
104a
106a
記憶回路情報・
中間データ復号化部
0
1
2
3
8
2-1
中間データ暗号化部
読み出し
書き込み
105
シミュレータ
エンジン

【図３】


回路情報
暗号化装置
暗号化部
供給
回路情報
暗号化復号化
ｱﾙｺﾞﾘｽﾞﾑﾃﾞｰﾀ
ｷｰﾃﾞｰﾀ
インターネット
HTTP
FTP
VPN
VPN
100
供給回路情報
復号化部
101
回路動作ｼﾐｭﾚｰｼｮﾝ装置

【図４】


回路情報
暗号化装置
暗号化部
供給
回路情報
暗号化復号化
ｱﾙｺﾞﾘｽﾞﾑﾃﾞｰﾀ
ｷｰﾃﾞｰﾀ
仲介者
HTTP、FTP
VPN
VPN
インターネット
VPN
VPN
HTTP、FTP
100
供給回路情報
復号化部
101
回路動作ｼﾐｭﾚｰｼｮﾝ装置

【書類名】　要約書

【要約】

【課題】　回路動作シミュレーション装置において、回路情報の秘匿性を高めつつ、容易にシミュレーションできるようにする。

【解決手段】　暗号化されて提供された回路情報（供給回路情報）は、供給回路情報復号化部１０１によって復号化され、さらに記憶回路情報暗号化部１０２により暗号化されて、記憶回路情報として記憶部１０３に記憶される。上記記憶回路情報は、記憶回路情報・中間データ復号化部１０４により復号化されてシミュレータエンジン１０５に入力され、シミュレーションが行われる。また、シミュレーション中の中間データは、中間データ暗号化部１０６により暗号化されて記憶部１０３に記憶され、やはり記憶回路情報・中間データ復号化部１０４により復号化されてシミュレータエンジン１０５に入力される。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　　大阪府門真市大字門真１００６番地
氏　名　　松下電器産業株式会社